UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

GRACE LAU, et al.,

Plaintiffs,

v.

GEN DIGITAL INC., et al.,

Defendants.

Case No. 22-cv-08981-RFL

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: Dkt. No. 52

The plaintiffs bring this consumer privacy action against Gen Digital Inc. and Jumpshot Inc. based on their data practices related to a browser extension, Avast Online Security & Privacy ("AOSP"). The plaintiffs allege that the AOSP browser extension is marketed to consumers as a way to stop third parties from tracking and colleting their data, and to stop malicious code that might try to steal their data. Allegedly, though, AOSP itself collected that same browsing data from users, and then used the browsing data for its own financial benefit by transmitting it to third-party advertisers.

On September 13, 2023, the Court issued an order dismissing some of the plaintiffs' claims. On November 27, 2023, the case was reassigned to the undersigned judge. After the plaintiffs filed a First Amended Complaint, the defendants moved to dismiss for lack of standing and failure to state a claim. The motion to dismiss is **GRANTED IN PART AND DENIED IN PART**. The plaintiffs do not state claims for wiretapping, because the alleged wrong is not an interception by a third party, but instead AOSP's alleged misuse of data that the plaintiffs sent to it. Nor do the plaintiffs state valid claims for violations of California's Unfair Competition Law or civil theft statute, because the plaintiffs have not lost "property" under those laws. However, the plaintiffs do state claims for invasion of privacy and an intrusion upon seclusion, as well as

unjust enrichment. The ruling assumes the reader is familiar with the facts, the applicable legal standard, and the arguments made by the parties.

Request for judicial notice. The defendants request that the Court find that two screenshots of privacy prompts displayed to users seeking to download AOSP from the Google Chrome Web Store and the Microsoft Edge Web Store are incorporated by reference into the FAC. (Dkt. No. 53 ("RJN").) A document is properly incorporated by reference "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *United States v. Ritchie*, 342 F.3d 903, 907 (9th Cir. 2003). "'Extensively' . . . should, ordinarily at least, mean more than once." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1003 (9th Cir. 2018) (quoting *Ritchie*, 342 F.3d at 907). Here, the defendants acknowledge that "the FAC does not specifically cite these privacy notices" (RJN at 3), and the plaintiffs question whether the privacy prompt in the screenshots is the same as any the plaintiffs may have encountered when they downloaded AOSP years ago (Dkt. No. 56 ("Opp.") at 9 n.3). The request for incorporation by reference is therefore **DENIED**.

Wiretapping claims. The plaintiffs fail to state claims for violation of the Electronic Communications Privacy Act and the California Invasion of Privacy Act because the defendants were a party to the alleged communications. The allegations in the FAC do not cure the fundamental defect identified by the Court's dismissal of the wiretapping claims in the original complaint: "Plaintiffs downloaded the extensions to monitor their browsing activity and have not alleged how the extensions could function without Defendants' participation in the communications." (Dkt. No. 45 at 7.) The Norton browser extension alleged in the FAC supports that AOSP perhaps could have *stored* less user information, but the FAC makes clear that even the Norton extension must read URLs to "check" them against its "blacklist." (*See* FAC ¶¶ 76, 79.) Similarly, the allegations about AOSP's usage of cookies speak only to how user information is catalogued and stored, not the initial interception of that information. (*Id.* ¶ 80 (alleging how cookies transmit data "intercepted, collected, and stored" by AOSP").) The wiretapping statutes, however, are directed at the unauthorized *interception* of communications,

not any subsequent storage and/or use. *See* 18 U.S.C. § 2511(1)(a)–(e) (prohibiting the unauthorized "interception" of an "electronic communication"); Cal. Pen. Code § 631(a) (prohibiting any person from using electronic means to "learn the contents or meaning" of any "communication" in an unauthorized manner).

To avoid application of the party exception, the plaintiffs also argue that the defendants should be treated as third parties, because the plaintiffs' communications were with the AOSP browser extension and AOSP allegedly did not need to "duplicat[e]" and transmit those communications to the defendants. (Opp. at 7–8.) But the cases on which the plaintiffs rely for this contention are distinguishable. In those cases, the plaintiffs thought they were sharing their information with solely the website operators, but unbeknownst to the plaintiffs, the website operators had allegedly embedded third-party code in their websites, which was transmitting the plaintiffs' information to a separate company that had created the embedded code. The question in those cases was whether the code creators should be treated as extensions of the website operators (and thus parties) or as third parties. *See, e.g.*, *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 899–900 (N.D. Cal. 2023) (finding that ActiveProspect, a software provider, was a third party to communications between the plaintiffs and Assurance IQ, LLC, an insurance website operator that had embedded ActiveProspect's code in its website).

By contrast, there is no unknown third party here. AOSP is the defendants' product, and the plaintiffs in this case chose to install that product with the expectation that AOSP would have access to the plaintiffs' browsing activity to provide a more secure browsing experience. (FAC ¶¶ 5, 37–39, 135–39, 143, 150, 156.) That AOSP allegedly did not work in the manner that the plaintiffs' expected does not change the fact that the defendants, as the operators of AOSP, were known parties to the alleged communications.

The motion to dismiss the ECPA and CIPA claims are therefore granted.

Invasion of privacy and intrusion upon seclusion. The FAC plausibly pleads claims for invasion of privacy under the California Constitution and intrusion upon seclusion. These claims have similar elements, and when considering them together, courts assess whether the plaintiff

has pleaded (1) a reasonable expectation of privacy and (2) whether the intrusion was highly offensive. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). In analyzing reasonable expectations of privacy, courts look to the totality of the circumstances. "[C]ourts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities." *See Facebook Tracking*, 956 F.3d at 602 (citing *Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d 633, 655 (Cal. 1994)).

The FAC's allegations about the amount of browsing data collected, the sensitive nature of some of that data (i.e., health information), and how the defendants gained access to that data through their representations about ASOP sufficiently allege a reasonable expectation of privacy. The FAC alleges that the plaintiffs used AOSP expecting it to "help protect" their privacy while browsing the internet. (FAC ¶¶ 135, 139, 143, 150, 156.) The defendants allegedly touted AOSP as having many "privacy features," including "Anti-tracking – prevent tracking on every website you visit" and "Global Privacy Control – stop web companies from collecting and selling your personal data." (*Id.* ¶ 38.) AOSP, however, allegedly did exactly what it represented it would protect against: AOSP collected, stored, and transmitted user browser information to third-party advertising partners for "targeted advertising, to the financial benefit of [the defendants]." (*Id.* ¶ 80; *see also id.* ¶¶ 71, 81, 84, 97–98, 133.)[1] The alleged information collected included "internet search engine keyword searches, search results, email inbox searches, browsing histories, video viewing histories, and [protected health information]." (*Id.* ¶ 8; *see also id.* ¶¶ 85–103.) From this information, the defendants could allegedly "recreate a user's entire web browsing history." (*Id.* ¶ 41.) The FAC further alleges that another browser security extension performed the same privacy functions as AOSP without tracking and collecting its users' information. (*Id.* ¶¶ 76–79.)

[1] Though the plaintiffs' allegations on how the information is shared with third-party advertisers are not a model of clarity, they are sufficient for notice pleading purposes. Although the defendants argue that they do not have the incentive to transmit the data to third-party advertisers in the manner alleged, that is a fact question that cannot be addressed on a motion to dismiss.

Thus, in view of the defendants' representations that ASOP was a browser security extension, the plaintiffs plausibly allege that a user reasonably would have expected that ASOP would not engage in mass collection of their data to be sent to others for the defendants' financial benefit.[2] As for the "highly offensive" element of the privacy claims, the FAC's allegations are sufficient to withstand dismissal at this stage. *Facebook Tracking*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."). The plaintiffs therefore plausibly allege claims for invasion of privacy and intrusion upon seclusion.

That is consistent with the Court's holding in its prior order. (*See* Dkt. 45 at 8–9 (relying on *Facebook Tracking*, 956 F.3d 589 (9th Cir. 2020)). In an attempt to revisit that holding, the defendants argue that the collection and storage of data cannot constitute an injury-in-fact for purposes of Article III standing, citing *Phillips v. U.S. Customs & Border Protection*, 74 F.4th 986 (9th Cir. 2023). The Ninth Circuit in *Phillips* observed that "the retention of records *alone* does not constitute a concrete injury," *id.* at 992 (emphasis added), but such retention may do so if the retention amounts to a harm "traditionally recognized as providing a basis for lawsuits in American court," like "intrusion upon seclusion," *id.* (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021)). Here, as described above, the FAC alleges a highly offensive intrusion into the plaintiffs' privacy, which is more than just the mere retention of data. As *Phillips* recognized, an "invasion of privacy" is "an injury identified by the Supreme Court as concrete."

[2] Though the defendants correctly observe that courts have traditionally not found a reasonable expectation of privacy in bank records or phone records disclosed to third party providers, the aggregation of data over time to create a detailed profile presents a different issue. *See Carpenter v. United States*, 585 U.S. 296, 314 (2018) ("There is a world of difference between the limited types of personal information addressed in [bank and phone records] and the exhaustive chronicle of location information casually collected by wireless carriers today."). Moreover, California courts have rejected the notion that disclosure to a third party automatically nullifies any expectation of privacy. "[P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic . . . . The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone." *Sanders v. Am. Broad. Companies, Inc.*, 978 P.2d 67, 72 (Cal. 1999).

Id. at 993 (noting "many other cases" finding standing based on retention of data "because the retention amounted to an invasion of [plaintiffs'] privacy interests").

Nor can the defendants escape liability by arguing that there is no "intrusion" because the plaintiffs allegedly gave the defendants access to the browsing data by choosing to install AOSP. Although the plaintiffs may have expected their browsing data to pass through AOSP for the software to perform its required functions, they allegedly did not expect for AOSP to collect and store extensive dossiers of their browsing data that could later be sold to third-party advertisers. *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014), presents an analogous situation. In that case, the plaintiffs had downloaded the defendants' applications and permitted the applications to "find friends" by scanning the plaintiffs' address books on their smartphones. *Id.* at 1060. In suing the defendants, the plaintiffs alleged that the defendants "obtained [the plaintiffs'] consent by misrepresenting [the apps'] purpose." *Id.* The plaintiffs allegedly "would not have consented had they known that the apps would not only scan their address books to determine whether their friends were using the same app, but then upload the address books to the app developer for other purposes." *Id.* Based on these allegations, the court concluded that the plaintiffs stated a valid claim for intrusion upon seclusion and denied the defendants' motion to dismiss. *Id.*

Similar to the *Opperman* plaintiffs, the plaintiffs here plausibly allege that they did not surrender their expectation of privacy in their browsing data by installing the AOSP browser extension. Each of the plaintiffs alleges that they would not have allowed AOSP to access their data at all if they had "known that [defendants] were invading [their] privacy" in the manner described. (FAC ¶¶ 135, 139, 143, 150, 156.) The FAC thus plausibly alleges an intrusion based on the defendants' access to the plaintiffs' extensive private browsing data, which the plaintiffs would not have provided had they known that the defendants would allegedly store and share the data in contravention of their reasonable expectations. *See Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1270 (9th Cir. 1998) (reversing grant of summary judgment for defendant employers on invasion of privacy claim where the plaintiff employees agreed to give

blood and urine samples for an employment-related health exams without realizing that the defendants would conduct additional intrusive medical and genetic testing on those samples for syphilis, pregnancy, and sickle cell traits); *Sanchez–Scott v. Alza Pharm.*, 103 Cal. Rptr. 2d 410, 419 (Ct. App. 2001) (reversing dismissal of intrusion upon seclusion claim where doctor allegedly obtained plaintiff's consent to a breast examination in front of a drug salesperson without disclosing the salesperson was not a medical professional).

The motion to dismiss the invasion of privacy and intrusion upon seclusion claims is therefore denied.

UCL. The plaintiffs fail to allege economic injury as required to bring a claim under the UCL. The FAC alleges three theories of injury: (1) "the unauthorized interception, collection, storage, use, and sharing of their personal information"; (2) diminution in value of the plaintiffs' private data; and (3) benefit of the bargain. (FAC ¶¶ 119–34, 277.)

Regarding the first theory, the misappropriation of private information alone does not constitute economic injury, as the Court explained in the prior order. (Dkt. No. 45 at 11–12.) *See Moore v. Centrelake Med Grp., Inc.*, 299 Cal. Rptr. 3d 544, 566 & n.13 (Ct. App. 2022) (finding unpersuasive federal cases that held that a loss of privacy in one's information was sufficient to allege UCL standing).

Next, the diminution-in-value theory is not plausibly alleged. The plaintiffs allege that they share their personal information with companies via consumer surveys in exchange for "rewards" and other "prizes" but the "value of [their] participation is decreased due to the fact that Defendants make available extensive information about [the plaintiffs'] consumer preferences and activity without paying [them]." (FAC ¶¶ 146–47, 153–54, 159.) Those allegations demonstrate that the plaintiffs are still able to participate in a market for their personal information; the allegations regarding the diminished value of their information are entirely conclusory, as the complaint does not allege facts supporting that the plaintiffs have not been able to capture the full value of their information as a result of the defendants' alleged conduct. *See, e.g., Moore*, 299 Cal. Rptr. 3d at 564 (concluding that diminution-of-value theory

was insufficient to support UCL standing where the plaintiffs did not allege "that any prospective purchaser of their PII [personal identifying information] might learn that their PII had been stolen in this data breach and, as a result, refuse to enter into a transaction with them, or insist on less favorable terms").

Lastly, the plaintiffs' benefit-of-the-bargain theory fails because AOSP was free, and, to the extent that the plaintiffs gave their information to AOSP in exchange for use of the browser extension, there is no plausible allegation that this transmission caused their information to diminish in value, as explained above. *Wesch v. Yodlee, Inc.*, No. 20-cv-05991-SK, 2021 WL 1399291, at *6 (N.D. Cal. Feb. 16, 2021) (holding that plaintiffs had not alleged that they "surrender[ed] more or acquir[ed] less in a transaction than they otherwise would have" for purposes of UCL standing where they had not paid money to the defendant).

The motion to dismiss the UCL claim is therefore granted.

Larceny. The plaintiffs still do not state a claim for statutory larceny because the browsing data is not "property" capable of theft under California Penal Code Section 496, for the reasons stated in the Court's prior order. (Dkt. No. 45 at 12-13.) Under California law, "property" must be "capable of exclusive possession or control." *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 902–03 (9th Cir. 1992) (summarizing California law). By its nature, browsing data is shared with a variety of service providers that facilitate access to the website at issue. To be sure, users have a strong privacy interest in controlling access to the aggregation of that data over time, as discussed above. But that data is not capable of *exclusive* possession or control. *See Tanner v. Acushnet Co.*, No. 823CV00346HDVADSX, 2023 WL 8152104, at *10 (C.D. Cal. Nov. 20, 2023) (collecting cases and noting that the "weight of authority holds that a plaintiff's 'personal information' does not constitute property").

Unjust enrichment. A claim for unjust enrichment is essentially a claim for restitution, the elements of which are that the defendant received and unjustly retained a benefit at the plaintiff's expense. *See Durell v. Sharp Healthcare*, 108 Cal. Rptr. 3d 682, 699 (Ct. App. 2010) ("Unjust enrichment is synonymous with restitution."); *Stark v. Patreon, Inc.*, 635 F. Supp. 3d

841, 857 (N.D. Cal. 2022). The FAC alleges that the defendants "produce[d] revenue" from the data that they allegedly improperly obtained from the plaintiffs. (FAC ¶ 284.) The defendants allegedly gained "financial benefit" by sharing that information with their third-party advertising partners for "targeted advertising." (*Id.* at 80.) These allegations are sufficient to state a claim for unjust enrichment. The motion to dismiss the unjust enrichment claim is therefore denied.

Statute of limitations. As noted in the prior dismissal order, Plaintiff Christopher Karwowski's invasion of privacy and intrusion upon seclusion claims are subject to a two-year statute of limitations.[3] (*See* Dkt. No. 45 at 4 (citing *Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 598–99 (N.D. Cal. 2021)).) The original complaint in this action was filed on December 19, 2022 (*see* Dkt. No. 1), so claims accruing prior to December 19, 2020, are untimely unless an exception applies.

To the extent the non-statutory privacy claims arise out of the alleged Jumpshot conduct, those claims are time-barred. The plaintiffs allege that Avast licensed its users' data to Jumpshot and knew Jumpshot was selling the data to third parties, and that this scheme was publicly exposed in 2019 and early 2020. (*See* FAC ¶¶ 53–57, 70, 174–75.) Although the plaintiffs argue that their claims about the Jumpshot conduct are preserved based on fraudulent concealment, the Court's prior order dismissed the claims as untimely because the plaintiffs "have not satisfied their burden" to allege such concealment. The FAC does not cure that deficiency. There continues to be no allegation that the defendants denied the Jumpshot conduct or lied about shutting down Jumpshot.

However, to the extent the privacy claims are based on a new scheme under which the defendants allegedly "secretly harvest[ed] data even after shuttering Jumpshot" in early 2020 (*id.* ¶ 169), the Court cannot find that Karwowski's claims are time-barred as a matter of law at this stage. "[A] complaint cannot be dismissed unless it appears beyond doubt that the plaintiff can

[3] The Court does not address the defendants' statute of limitations arguments regarding Korwowski's wiretapping claims or plaintiff Grace Lau's CIPA claim, as those claims are dismissed for independent reasons discussed above.

prove no set of facts that would establish the timeliness of the claim." *See Supermail Cargo, Inc. v. United States*, 68 F.3d 1204, 1206 (9th Cir. 1995). The FAC alleges only that Karwowski used AOSP "from 2019-2020." (*Id.* ¶ 139.) It is thus not apparent from the face of the FAC that the applicable statute of limitations has run, as the FAC does not preclude the possibility that Karwowski used AOSP after December 19, 2020.

Moreover, the plaintiffs plausibly allege that the discovery rule applies to Karwowski's non-Jumpshot claims prior to December 19, 2020. To rely on the discovery rule for delayed accrual of a cause of action, a plaintiff must plead facts showing (1) the time and manner of discovery and (2) the inability to have made earlier discovery despite reasonable diligence. *Fox v. Ethicon Endo-Surgery, Inc.*, 110 P.3d 914, 920–21 (Cal. 2005). The FAC alleges that Karwowski had no basis to suspect or discover the defendants' continued tracking, collecting, and sharing of AOSP user information until he first consulted with counsel in September 2022. (FAC ¶ 167.) That allegation is plausible based on the technical nature of AOSP's operation and the defendants' alleged statements about protecting user privacy after Jumpshot's shuttering, including that "any practices that jeopardize user trust are unacceptable." (*Id.* ¶ 174.) These allegations are sufficient at this stage to preclude dismissal of the claims as untimely.

The motion to dismiss Karwowski's non-statutory privacy claims is therefore granted to the extent those claims are based on Jumpshot's alleged conduct and is otherwise denied.

Leave to amend. The dismissed claims in the FAC suffer from the same deficiencies as those dismissed in the original complaint. As the plaintiffs were already granted leave to amend once but were unable to cure the identified defects, the Court finds that further leave to amend would be futile. *See Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990) ("The district court's discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint.").

Based on the foregoing, the motion to dismiss is **DENIED** as to the claims for invasion of privacy, intrusion upon seclusion, and unjust enrichment, and otherwise **GRANTED WITHOUT LEAVE TO AMEND**.

An initial case management conference is set for **May 1, 2024**, **at 10:00 a.m. via videoconference**. The parties shall file a joint case management statement by **April 24, 2024**.

IT IS SO ORDERED.

Dated: April 3, 2024

RITA F. LIN
United States District Judge